



Report of the State Comptroller of Israel | Cyber and  
Information Systems | 2022

The Israel Tax Authority

---

# **Cyber Protection and Business Continuity in the Automated Processing Service Unit at the Tax Authority**





## Cyber Protection and Business Continuity in the Automated Processing Service Unit at the Tax Authority

### Background

The Automated Processing Service (Shaam) is a unit serving the Israel Tax Authority's IT (Information technology) system and providing it through computer services for collection and enforcement, creating proper deterrence and exhaustion of taxpayers' rights. Shaam serves about 1.3 million "customers": companies, other types of corporations, self-employed, controlling stakeholders, employees, and recipients of work grants, employees performing tax adjustments and tax refunds, 6,000 employees of the Tax Authority, 13,000 representative offices, and 7,000 lawyers. Shaam manages hundreds of projects every year, from projects for immediate execution to long-term projects. Shaam keeps the information about citizens, taxpayers, dealers, and other entities in its systems.

The law of Security in Public Bodies, 1998 determines the areas of authority and responsibility for physical security, information security, and the security of essential computer systems of various public bodies, including government and privately owned bodies. The law defines critical computer systems as "computer systems determined as essential by the body authorized to that by the government".

In 2010, a senior steering committee decided that Shaam would be included in the Second and Fifth Schedules for the Regulation of the Law of Security. Accordingly, the National Cyber Directorate was authorized to issue Shaam professional guidelines concerning securing essential computing systems.



## Key figures

**1.3 million**

Shaam service recipients: companies, corporations, self-employed, employees, and more

**part**

of the Shaam employees who require security clearance do not have the required clearance

**11**

the number of findings of the penetration test conducted by an external consultant on behalf of the State Comptroller's Office

**2014**

the year in which the preparation of a business continuity plan began in Shaam and has not yet ended

## Audit actions



From November 2021 to February 2022, the State Comptroller's Office examined Shaam's information security and cyber protection. The audit was conducted at Shaam, and completion examinations were carried out in the National Cyber Directorate.

The audit included the examination of some aspects of cyber protection, the penetration test of the system supporting a business process at the Tax Authority (System A), and Shaam's preparedness for business continuity and disaster recovery.

This report was submitted to the Prime Minister on July 31, 2022, and was classified as confidential until its discussion at the State Audit Committee's Subcommittee.

Under the authority vested upon the State Comptroller in Section 17(c) of the State Comptroller's Law, 1958 [Consolidated Version], considering the government's reasoning, consulting with the bodies entrusted with the security of defense information, in coordination with the Knesset chairman, and as the said subcommittee did not convene, it was decided to publish this report while classifying as confidential parts thereof. These parts were not brought before the Knesset and will not be published.

The audit report's findings and recommendations are correct as of the aforementioned date of its publication.



## Key findings



**The steering committee's duties over critical computing infrastructures** – it was raised that the committee's responsibilities were defined in the letter of appointment in general terms and were not detailed as required by the regulatory guidelines. Moreover, the committee's discussions do not address the actions it should take according to its duties, as the guidelines require.



**Mapping processes and information assets** – according to the regulatory guidelines, Shaam should map the information assets and access routes to comply with a security plan. Gaps were found in mapping the processes and information assets carried out at Shaam, which does not fully comply with the regulatory guidelines' requirements.



**Discrepancies in Shaam procedures** – the audit found discrepancies in the regulatory guidelines in some Shaam procedures, among other things, regarding the work interface with the National Cyber Directorate.

- **Changes management** – no reference was found in the relevant procedure to the need to update the appropriate party and include it in analyzing the risks and expected effects of the changes, as required by the guidelines.
- **Procedure for handling information security incidents** – there is a procedure at Shaam but it does not refer to the obligation to report to the relevant party and the need to include it in the incident's investigation. In addition, there is no reference pertinent to an area required in the guidelines.



**Centralization of information regarding the supply chain** – gaps were found regarding the information collected by the Shaam Information Security Wing on the supply chain. Furthermore, Shaam did not use the supply chain module in the dedicated system developed by the National Cyber Directorate.




**Weakness in a particular server** – there were gaps in the control of a specific server.




**Required clearance** – the audit raised gaps between the clearance approval level needed according to some Shaam employees' duties and their level of approval in practice.




## Penetration test on behalf of the State Comptroller's Office on System A


-  This system supports a business process at the Tax Authority. During the test, findings emerged that endangered the information from a business point of view and the organization's reputation.

## Preparedness for business continuity and disaster recovery

-  **Regulation of the wing's activities** – in November 2016, Shaam's director decided to form an organizational structure that will be planned, with the assistance of consultants, to establish a quality and business continuity wing. The Civil Service Commission stipulated the wing approval of its necessity by the ICT Authority. It was raised that the wing has been operating since the end of 2016, although the Commission has not approved the organizational structure change. The job definitions of the wing employees are the definitions of their previous positions, and they are employed according to the headcounts assigned to other wings. Consequently, the wing authority and its duties are not regulated.






-  **Disaster recovery plan** – the disaster recovery plan includes a plan for the recovery of the technological array, the process of activating emergency mode, the process of coming back from emergency mode to routine, the emergency drills, and the main indices for recovery:

- Return Point Objective (RPO) – the volume of information lost during a disaster.
- Return Time Objective (RTO) – the maximum time from the moment the decision is made until the emergency site is activated.
- Gaps were found regarding the completion of a disaster recovery plan.

-  **Business continuity plan** – gaps were found in formulating a business continuity plan and in its completion.



## Key recommendations

-  It is recommended that Shaam rectify the deficiencies found in mapping the processes and the information assets.
-  It is recommended that Shaam update its procedures and include all the necessary actions according to the regulatory guidelines.
-  It is recommended that Shaam use the dedicated system developed by the National Cyber Directorate to examine the supply chain.
-  It is recommended that Shaam ensure that the clearance level of all Shaam employees is adapted to their positions.
-  It is recommended that Shaam examine the findings of the penetration test conducted on behalf of the State Comptroller's Office and rectify the deficiencies raised in this report.



---

---

## Summary

Shaam is the Tax Authority's IT body. Hence, it develops information systems, maintains existing systems, and holds information. It is of great importance that Shaam will have a high level of cyber protection, that functions fully in times of crisis, and rapidly recover from disaster.

By the audit findings, Shaam should improve the cyber protection of its systems.

It is recommended that Shaam rectify the deficiencies raised in this report as soon as possible and consider the implementation of the report's recommendations.